UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT GREENEVILLE

UNITED STATES OF AMERICA	)	
	)	
V.	)	NO. 2:08-CR-33
	)	
JEFF F. TILLOTSON	)	

REPORT AND RECOMMENDATION
REGARDING MOTIONS TO SUPPRESS EVIDENCE (DOCS. 41, 67)

The defendant has filed two motions to suppress (Docs. 41 and 67), in which he asks that all evidence seized as the result of the execution of a search warrant at his residence on November 6, 2007, be suppressed. The search warrant was issued by this court. These motions have been referred to the United States Magistrate Judge under the standing orders of this Court and pursuant to 28 U.S.C. § 636(b). An evidentiary hearing was held on November 6, 2008.

BACKGROUND

Having evidence that a computer located at 1240 Catawba Street in Kingsport, Tennessee, was being used to upload and download images of child pornography, Special Agent Michelle Evans of the Bureau of Immigrations and Customs Enforcement requested and was granted a warrant from this court to search that premises for the following evidence: all computers and electronic data storage devices which could store images of minors

engaged in sexually explicit conduct; all records pertaining to the possession or distribution of child pornography; books and magazines containing child pornography; photographs and negatives thereof, including copies, of child pornography; all movies (films, video cassettes, and DVD's) of child pornography; records, correspondence, etc. involving offers to transmit child pornography, or that identified persons transmitting child pornography, whether by US mail or by computer; all records, etc. that involved the transmission of child pornography, whether by mail or by computer; all records, etc. that concern the preparation and acquisition of names regarding the distribution of child pornography in interstate commerce, whether by mail or by computer; any records that contain the names and address of minors engaged in sexually explicit conduct; records of internet usage, including user names, e-mail addresses, etc., used for the purposes of communication on the internet.

DEFENDANT'S MOTIONS

Defendant argues that (1) the scope of the warrant was over-broad, thus converting into a prohibited general warrant; (2) the warrant was not supported by probable cause, and it authorized the seizure of items for which there was no probable cause; (3) the information relied upon by the magistrate judge in issuing the warrant was stale; (4) the actual search of the defendant's computer and hard drive exceeded the scope of the warrant; (5) the methodology used in executing the search of defendant's computer was unreasonable and over-broad, and was not designed to minimize unwarranted intrusion on the defendant's privacy; (6) the warrant violated the particularity requirement of the Fourth Amendment

because the warrant was without limitation regarding the items to be seized; (7) the United States searched and seized data from the computer after the warrant had expired, in violation of Rule 41; (8) the affidavit failed to demonstrate the reliability of the source of information tying the IP address to defendant's residence; and (9) the warrant failed to tailor its search appropriately when the United States was aware that there were multiple families residing in the residence at 1240 Catawba Street in Kingsport.

WAS THE WARRANT OVER-BROAD AND THUS A GENERAL WARRANT?

Defendant rightly argues that the "particularity requirement" of the Fourth Amendment proscribes general warrants. *See, United States v. Gardiner*, 463 F.3d 445, 471 (6th Cir. 2006). In his brief, defendant makes this assertion: "The warrant left it up to the discretion of the officers conducting the search to decide which items were obscene."[1] If that statement were correct, defendant would have a valid point. However, the warrant did not authorize the executing officers to search for "obscene" materials; the warrant directed the officers to search for evidence involving minors engaged in sexually-explicit conduct, i.e., child pornography. Nowhere is the word "obscene" used in the warrant. For that matter, neither does it appear in the affidavit or application.

"Minors engaged in sexually explicit conduct" is self-defining, but to the extent more is needed, the warrant described the evidence to be seized as "images of minors engaged in

[1]Brief, Doc. 42, p. 9.

sexually-explicit conduct as defined in Title 18, United States Code, Section 2256."

The executing officers had no discretion regarding the evidence for which they were searching and ultimately to seize, and thus the warrant was not over-broad.

WAS THE SEARCH WARRANT SUPPORTED BY PROBABLE CAUSE? WAS THE INFORMATION PROVIDED IN THE AFFIDAVIT STALE?

The affidavit recited that on September 16, 2007, at approximately 10:25 p.m. (Pacific Time) Special Agent Mooney of Immigration and Customs Enforcement connected to the internet from his computer in Portland, Oregon. He entered a chat room that was devoted to child pornography. Once in that chat room, Agent Mooney came across an advertisement from a person using the nickname "MovServ." That advertisement stated that MovServ had images of child pornography he was willing to trade in exchange for other images of child pornography. Agent Mooney connected to MovServ's fileserver, and he reviewed the available files for downloading. At 10:32 p.m., he retrieved a video snippet, seventeen seconds in length, that depicted child pornography. He downloaded three more video clips of child pornography, the last being at 10:38 p.m.

Agent Mooney noted that the MovServ file server had the Internet Protocol address of 24.158.106.51. Using an internet database named "maxmind.com," Agent Mooney learned that the IP address 24.158.106.51 was assigned to the Internet Service Provider, Charter Communications.

The following day, September 17, Agent Mooney submitted a summons to Charter

Communications, asking for subscriber information related to the IP address 24.158.106.51 during the time of his session with MovServ, which of course would have been on September 16, from 10:15 p.m. through 10:38 p.m.

On September 25, 2007, Charter Communications responded to Agent Mooney's summons by advising him that the subscriber for that address was Joann Lukes at 1240 Catawba Street in Kingsport.

On October 17, 2007, using a law enforcement data base, Special Agent Evans (the affiant) learned that Joann Lukes was Joann Lubrano, a/k/a Joanne Tillotson, residing at 1240 Catawba Street in Kingsport.

Agent Evans submitted her application and affidavit to this magistrate judge on November 5, 2007, and the warrant was issued that same day. In was executed the following day.

Based on Agent Evans' affidavit, this magistrate judge believed, and still believes, that probable cause existed to believe that a computer located at 1240 Catawba Street in Kingsport was being used to upload and download child pornography.

Defendant argues that the information provided in Special Agent Evans' affidavit submitted to this court was stale. In this regard, he points out that Agent Mooney downloaded child pornography on September 16, yet Agent Evans applied for the warrant on November 5.

There is no arbitrary or bright-line time limitation that determines whether information submitted in support of a search warrant is stale; it depends upon the nature of the crime, the

place to be searched and the things to be seized. *United States v. Spikes*, 158 F.3d 913, 923-24 (6th Cir. 1998). Approximately six weeks elapsed between the time Agent Mooney downloaded child pornography from the MovServ file server to the time this court issued its search warrant for any computers at 1240 Catawba Street in Kingsport, Tennessee. Based on the advertisement posted by MovServ and read by Agent Mooney, it was apparent that MovServ was engaged in an on-going enterprise involving the trading of child pornography. It was unlikely in the extreme that it was an isolated circumstance of brief duration. Rather, it was far more likely that it was of indefinite duration. The information not only was not stale, under the circumstances it was extremely fresh.

DID THE SEARCH OF DEFENDANT'S COMPUTER AND HARD DRIVE EXCEED THE SCOPE OF THE WARRANT?

Defendant's argument is a bit hard to follow. Although he acknowledges that " a computer may be seized because it is itself evidence," he also says that he had "an expectation of privacy in the contents separate from that in the computer itself."[2]

Respectfully, the computer "itself" would be evidence only if it had been stolen. Rather obviously, it is the *contents* of a computer that is the evidence in crimes involving computers. With regard to child pornography, it is self-evident that it is the contents of the computer - the files - that is the evidence.

The Fourth Amendment to the Constitution provides that search warrants must

[2]Brief, Doc. 42, p. 12.

particularly describe the place to be searched, and the persons or things to be seized. This of course is the "particularity requirement." *See, e.g., Mapp v. Ohio*, 367 U.S. 643, 655 (1961). The items to be seized pursuant to a warrant must be described with sufficient particularity to prevent the seizure of one thing under a search warrant that describes another thing. *See, Coolidge v. New Hampshire,* 403 U.S. 433, 461 (1971). However, the specificity required in a warrant is not amenable to an absolute or bright-line definition; it varies from case to case, depending upon the type of items to be seized and the type of crime under investigation. A warrant need only be "as specific as the circumstances and the nature of the activity under investigation permit." *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988).

The advent of the computer age, and the explosion of electronically-generated and stored information makes one appreciate why the particularity requirement must be flexible in light of the nature of the case. Once upon a time, not so many years ago, pornography consisted of images on paper, i.e., photographs. Of course, there undoubtedly were movies (on film) depicting pornography, and sometime later movies on video tapes. All such material - photographs, (magazines), movies, and video tapes - were distributed in the "plain brown envelopes" through the mail, or in the back rooms of adult book stores. But the electronic age has changed the landscape completely. The printed photographs, filmed movies and video tapes have been replaced by digital electronic information, and is communicated from computer to computer, state to state, and country to country, more or less instantly. Child pornography not only is communicated in electronic form, it is stored

in electronic form. It is the manner of that storage that dictates the scope of search warrants for electronically-stored information. Files on computers containing child pornography likely would not be identified as "My Child Porn;" rather, knowing that pornographic depictions of minors are highly illegal, the owner would be expected to store the data in innocuously-named files. To search for specific data on a computer, such as child pornography, or data concerning child pornography (correspondence, e.g.), it is necessary to search basically every file on the computer.

To be sure, the warrant did not explicitly state that the officer should search "all files" on any computers at 1240 Catawba Street; rather, it said that the officer should search "all computers, including electronic . . . storage devices . . . ." If one should gather together one hundred people of moderate intelligence with only a modicum of computer knowledge, and then tell them that they should "search a computer for child pornography," all one hundred of them would immediately understand that they were to search the *contents*, i.e., the files, on that computer in an effort to locate the child pornography.

The warrant was not over-broad, and it was not a general warrant. Every item to be seized had one common element: images or depictions of minors engaged in sexual conduct. Thus, the warrant was sufficiently particular, and limited, in light of the nature of the evidence and where it was likely secreted. Similarly, the search itself did not exceed the scope of the warrant.

WAS THE SEARCH METHODOLOGY UTILIZED BY THE AGENTS

UNREASONABLE AND OVER-BROAD, AND NOT DESIGNED TO MINIMIZE UNWARRANTED INTRUSIONS ON THE DEFENDANT'S PRIVACY?

Defendant argues that the methodology used by the United States in executing the warrant did not minimize the intrusiveness of the search. He says that a search for computer files "does not permit the seizure of the computer any more than a warrant authorizing the search of a house for a murder weapon would permit the police to cart off the entire contents of the house." He goes on to argue that the United States could have searched the computer on-site and copied all files, or it could have made a "mirror image" of the entire hard drive. The problem with defendant's argument is that it ignores the realities of electronically-stored information, and the fact that a person with advanced computer skills could bury incriminating data so far in a computer that it cannot be easily found. Data can be obscured or hidden by placing it in files with misleading names, or even in files that suggest the contents are something completely different from what they actually are. In her affidavit, Agent Evans thoroughly explained why it would be necessary to remove the computer to a "controlled environment," i.e., a computer lab, before attempting to search the contents. Removing the computer off premises for analysis by a computer expert not only was reasonable, it was a necessity.

The methodology used to search the defendant's computer was reasonable.

DID THE WARRANT VIOLATE THE PARTICULARITY REQUIREMENT BECAUSE IT WAS WITHOUT LIMITATION ON THE ITEMS TO BE SEIZED?

Defendant argues that the United States was authorized "to seize all computer

equipment and software without limitation . . . [which is] nothing but a violation of the particularity requirement. Indeed, it did not even request to seize any particular file name or the like. It just wanted it all."[3]

To repeat, every item of evidence for which the warrant authorized the officer to search and seize on computers was that which depicted, contained, or involved child pornography as defined in 18 U.S.C.§ 2256. Recalling that pornography could be located in files with misleading names, authorizing a search of all files on the computer was as specific as the warrant could be under the circumstances. The warrant did not violate the particularity requirement.

DID THE GOVERNMENT SEIZE DATA FROM DEFENDANT'S COMPUTER AFTER THE WARRANT HAD EXPIRED, IN VIOLATION OF RULE 41?

This argument presents the question: When does a search end and analysis of the seized evidence begin?

Defendant's computer was seized on November 6, 2007. For some period of time thereafter, computer forensic experts analyzed the data files on that computer to determine if any of them contained images of child pornography or related evidence thereof. Defendant essentially argues that the United States had ten days to "search" the contents of his computer, after which time the United States' authority to do so expired under the terms of the warrant.

[3]Brief, Doc. 42, p. 17.

Defendant's argument ignores the realities of electronically-stored data and the difficulties which the United States confronts in locating that data on a computer. Indeed, Special Agent Evans addressed this difficulty in paragraph 36 of her affidavit filed in support of the application for the search warrant.

The subsequent analysis of the computer's contents is not a search in the sense contemplated by Rule 41 of the warrant.

DID THE WARRANT FAIL TO DEMONSTRATE THE RELIABILITY OF THE SOURCE OF INFORMATION TYING THE IP ADDRESS TO DEFENDANT'S RESIDENCE?

To repeat, Agent Mooney in Oregon had downloaded child pornography from a computer with an Internet Protocol address of 24.158.206.51. Using an internet database called "maxmind.com," which apparently is something of an internet address book, Mooney learned that this address had been assigned to Charter Communications. This address would be used by one of Charter's internet subscribers, or customers. Defendant argues that Agent Mooney failed to confirm that "maxmind.com" was a reliable source of information regarding the assignment of IP addresses.

The fallacy of defendant's argument is that maxmind.com merely advised Agent Mooney to which internet service provider this particular IP address had been assigned; in this case, Charter Communications. Had the information provided by maxmind.com been incorrect, then it follows that Agent Mooney would have contacted an incorrect internet service provider, which in turn would have been unable to comply with the summons

ultimately served upon it by Agent Mooney. For example, had maxmind.com incorrectly indicated that the internet service provider was Comcast, Comcast would have responded to Agent Mooney's summons by stating that the IP address of 24.158.106.51 was not assigned to it. Here, rather obviously, the information provided by maxmind.com was correct since Charter Communications identified the subscriber as Joanne Lukes at 1240 Catawba Street in Kingsport.

Through an expert witness, defendant presented evidence that suggested that the computer at defendant's residence had a "dynamic" IP address, not a static address. In other words, defendant's IP address *could* change from one internet session to another, and therefore the information provided by maxmind.com *could* have been incorrect. In this regard, the expert testified that maxmind's information tended to "degrade" 1.5 percent each month because of changing IP addresses. Defendant's argument is understood, but it is also rejected. Within the space of a few hours at the most, Agent Mooney conducted his "maxmind" query and learned that the IP address was assigned to Charter Communications. Charter Communications in turn advised that the subscriber for that IP address, for the time period in question, was Joanne Lukes of 1240 Catawba Street in Kingsport, Tennessee. Bearing in mind that even a 1.5 percent degradation in accuracy over the course of an entire month is virtually inconsequential, the chances that maxmind had incorrect information within the space of a few minutes or hours is virtually nil. If absolute certainty is required as defendant implicitly argues, then a court would *never* be able to rely on subscriber information regarding an IP address since in the vast majority of cases there would be a

chance that any IP address is dynamic and changing from time to time. The standard is *probable cause*, not absolute certainty.

In short, maxmind.com does not enter into the probable cause equation.

DID THE UNITED STATES FAIL TO PROPERLY TAILOR ITS SEARCH?

Defendant argues that 1240 Catawba Street was a multi-family home, and indeed it was. Defendant and his wife lived with defendant's mother and step-father. Defendant thus argues that the search warrant was not sufficiently "tailored" or limited, bearing in mind the number of people who lived at that address.

What defendant's argument overlooks is that the United States had probable cause to believe that a computer located in the residence at 1240 Catawba Street was being used to transmit and receive images of child pornography. As far as the United States knew, *any* of the occupants of 1240 Catawba Street - or all of them, for that matter - could have used the computer to send and receive child pornography. Having no knowledge where the computer (or computers) and other electronic storage devices might be located, Agent Evans reasonably was authorized to search throughout the entire house. By the same token, documents, records, and correspondence could be located anywhere within the house. The search warrant was as "tailored" as it could be under the circumstances.

DID AGENT MOONEY (IN OREGON) IMPROPERLY GAIN ACCESS TO PRIVATE STATISTICAL INFORMATION, INCLUDING THE PURPORTED IP ADDRESS WITHOUT AUTHORIZATION?

Defendant argues that Special Agent Mooney "accessed private statistical information that [was] not intended to be open to the public." He specifically refers to paragraph twenty of the affidavit.

Paragraph twenty of the affidavit reads:

> 20. After accessing the "MovServ" file server, SA Mooney reviewed the statistics maintained by the fileserver. Those statistics stated among other things, that the file server had 531 total files available for distribution, comprising 8.71 gigabytes of data, and had been visited by 31 different countries and had 4,721 uploads, comprising 8.41 gigabytes of data, and 6,856 downloads, comprising 6.36 gigabytes of data.

Absolutely no evidence was presented on this issue at the hearing, and neither was it addressed in argument. The court assumes that defendant takes the position that Agent Mooney "hacked" into the fileserver and read information that normally would be shielded from public view.

Paragraph twenty of the affidavit simply does not support the suggestion that Agent Mooney hacked into the fileserver and read "secret" information. It is more reasonable to conclude from paragraph twenty that the information is there to be read if the person seeking the information has the requisite knowledge to get it. In any event, paragraph twenty, even if utterly ignored, does not lessen the probable cause to believe that the fileserver was receiving and transmitting images involving child pornography.

THE SEIZURE OF THE MARIJUANA AND THE FIREARM

During the execution of the search warrant, the executing officers seized a firearm and

a quantity of marijuana. In his second motion to suppress (Doc. 67), defendant asks that this evidence also be suppressed for the same reasons set forth in his first motion to suppress.

The search warrant did not authorize the executing officers to search for firearms or illegal drugs. However, when an officer is executing a search warrant and sees in plain view an item which he believes constitutes evidence of criminal activity, he may lawfully seize that item. *United States v. Beal*, 810 F.2d 574, 577 (6th Cir. 1987).

The illegal character of the marijuana requires no discussion. Ordinarily, the illegality of the weapon would not have been immediately apparent, but it must be recalled that it was discovered in proximity to the marijuana. The marijuana and gun were discovered as the agents executed the search warrant. If the search warrant was valid, there is no basis to suppress evidence of the marijuana or gun.

CONCLUSION

In the opinion of this magistrate judge, the warrant was supported by probable cause and the information relief upon by the magistrate judge in issuing the warrant was not stale; the search of the defendant's computer and hard drive did not exceed the scope of the warrant; the methodology used in executing the search of defendant's computer was reasonable, and it did not unjustifiably intrude upon defendant's privacy; the executing officers had no discretion in what items to seize, and therefore the warrant did not violate the particularity requirement of the Fourth Amendment; the search did not extend beyond the time authorized in the warrant itself; the affidavit adequately demonstrated the reliability of

the information that tied the IP address to defendant's residence; and the warrant was reasonably tailored to the nature of the search itself. The marijuana and firearm were discovered in plain view during the execution of the warrant.

It is respectfully recommended that defendant's motions to suppress (Docs. 41 and 67) be denied.[4]

Respectfully submitted,

s/ Dennis H. Inman
United States Magistrate Judge

[4]Any objections to this report and recommendation must be filed within ten (10) days of its service or further appeal will be waived. 28 U.S.C. § 636(b)(1)(B) and (C). *United States v. Walters*, 638 F.2d 947-950 (6th Cir. 1981); *Thomas v. Arn*, 474 U.S. 140 (1985).